



**HIPAA**  
**(Healthcare Insurance Portability**  
**and Accountability Act)**

Self-Study Guide

## **OBJECTIVES**

By completing this self-study guide, you will gain a broad understanding of the Health Insurance Portability and Accountability Act (HIPAA): what it is, why it is important, and what it means to you.

Successful completion of this program will be accomplished by completing the examination on the last page of this self-study guide with a score of 80% or better.

## **INTRODUCTION**

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law by President Clinton on August 21, 1996. The Privacy Rule took effect in April, 2001 and most healthcare organizations had to meet the standards set by the rule by April 2003. Generally speaking, it was created to improve access to health insurance, to protect the privacy of healthcare information and to promote the standardization of electronic healthcare related records to improve and safeguard their use. To improve healthcare, HIPAA includes measures for standardizing how insurance claims are processed; for making sure health information is transmitted securely; and for protecting the privacy of patients. For purposes of this self study training guide, focus will be placed on the Privacy Rule and on security measures used to help keep information private.

## **DEFINITIONS**

Security Rule - pertains to information that is stored or transmitted electronically

Privacy Rule - covers certain health information in any form

Disclosure – giving out (the release, transfer or provision of access to) protected health information to persons or entities outside of the Hospital

Minimum Necessary Information – the least protected health information you “need to know” to do your job

Protected Health Information (PHI) – any information (oral, written, electronic, magnetic or recorded in any way) that applies to a patient’s health condition now, in the past or in the future

Reasonable Safeguards – the steps the Hospital and employees need to take to make sure patient information remains private.

## **PRIVACY RULE**

The Privacy Rule protects the privacy of patients by limiting how personal health information can be used; by requiring security of paper or electronic health records; and by informing patients of their rights.

The Privacy Rule allows patients to obtain a copy of their health records, ask for changes to their health records, and find out and limit how their personal health information may be used.

### **Frequently Asked Questions (FAQ)**

#### Protected Health Information

##### **1. How can I protect health information?**

By using the minimum necessary information rule, you can protect health information. Access only the information you need to use your job and when you need to share PHI with others, provide only the information the other person or organization needs.

##### **2. How does PCH limit access to information?**

PCH limits access to protected health information (PHI) by requiring that only people who need that information for treating patients should have access to patient files. In addition, staff in Health Information Management and the billing office should access minimum necessary information in order to process claims or requests for information. Other ways that PCH limits access to PHI is through the use of computer logins and passwords so that only certain information can be accessed by authorized staff. All employees have a part in limiting access to protected health information whether the information is oral, written, electronic, magnetic, or recorded in any way.

## **DISCLOSURE**

There are two situations in which you must disclose information: 1) the patient requests information about him/herself and 2) the Department of Health and Human Services needs it to find out if the Privacy Rule is being followed.

In general, you may disclose or use PHI for healthcare purposes:

- To treat a patient
- To obtain payment for healthcare services
- For quality assessment
- For competency (performance appraisal or accreditation)
- For fraud and compliance programs

- For management activities

In some cases, with patient approval, you can use or share information with family or friends. The patient has the right to limit how information can be shared. For example, the patient may say he or she does not want certain relatives to be given information about him or her. If you have any questions as to whether or not someone is permitted to receive patient information, check with your supervisor, before you disclose the protected healthcare information.

You may also disclose information in the following situations:

- If it is required by law, such as a court order
- To public health officials, in order to prevent or control disease
- In the case of abuse or domestic violence
- To help law enforcement officials find a suspect, material witness or missing person
- To notify law enforcement officials of a suspicious death
- To funeral director or coroners
- For the purpose of organ donation
- In the case of some government actions, such as military missions or security activities
- To provide information to meet workers' compensation laws
- To help in disaster relief efforts

In each of the above mentioned cases, you are allowed, but not required to share information and specific conditions apply. Check with your supervisor to determine if authorization is needed.

## **AUTHORIZATION**

### ***(To disclose information)***

Authorization is the permission a patient gives to allow PCH to use health information. Authorization must be in writing and specifies what information can be used, how the information can be used and for how long the information can be used. A patient may change his/her mind about authorization at any time.

It is important to know when authorization is required. Examples of when you must get authorization include providing information to an insurer or other entity for marketing purposes or before sending pre-employment physical results to an employer. If you have any questions about the when authorization is required, check with your supervisor.

Reminders (disclosure and authorization):

- When sharing information, use the minimum necessary information rule- access only the information you need and limit the information you disclose.

- Do not allow the fear that information will be disclosed get in the way of patient care!
- Take necessary steps to keep all information private.
- Answering machines – when leaving a message on an answering machine or a person other than the patient, be careful! It is best to simply ask the patient to return your call.

Some **Do's** and **Don'ts** when talking about patients:

**DO** speak quietly when possible.  
**DO** avoid the use of patient names in public areas.  
**DO** share information that is needed to treat the patient.

**DON'T** share PHI with others who do not need to know it.  
**DON'T** share PHI you are not authorized to disclose  
**DON'T** let privacy issues stand in the way of treating the patient properly

## FAQ

### *(Privacy and Disclosure)*

1. **Can a healthcare provider talk to a patient about their condition if they share a room with another patient?**  
Yes, but speak quietly to keep the information as private as possible.
2. **Can healthcare providers talk to each other about a patient's condition in the nurses' station?**  
Yes, but again, make every effort to keep the conversation private.
3. **What steps do I need to take to keep information private when I talk to patients?**
  - Talk quietly, lowering your voice when talking to patients. If the patient is hard of hearing, you may need to find a more private place to talk.
  - Try to talk to patients in a private place when possible. If you need to talk to a patient in a semi-private room, draw the curtain and lower your voice.
  - Limit what you say in public places such a lobby, waiting room, or cafeteria. Do not refer the patient's condition or the reason for the visit.

## **PROTECTING PRINTED PHI**

Printed protected healthcare information may be found in many places:

- Patient charts
- Wristbands
- Medicine bottles
- Diagnostic reports
- Census lists
- Billing statements, patient mailings
- Faxes or printed emails that contain patient information

Keeping printed PHI private:

- Lock filing cabinets or rooms containing PHI.
- All paper with PHI must be placed in the shred bins for shredding. **DO NOT** discard paper with PHI into the regular trash cans. Privacy rule may be viewed at [www.hhs.gov/ocr/privacy/index.htm](http://www.hhs.gov/ocr/privacy/index.htm).
- Fax only to secure locations or when there is someone there to receive it
- Turing paperwork upside down on counters or desks if there is a possibility that someone can read the information.

## **PROTECTING ELECTRONICALLY STORED INFORMATION**

Electronically stored PHI is any information which is stored or sent by computer. This includes patient databases, patient record and patient billing information stored on a computer on a hard drive, server, disk, CD, DVD, or other storage device (flash drive). The electronic transmission of patient healthcare information is covered under the security rule of HIPAA.

Ways to protect storing and transferring information include:

- Password protection – Do not share your password with anyone. Change the password often or if you feel it has been compromised.
- Log off the computer system when you leave the computer- even if you are just going to be “gone a minute”.
- Turn computer monitors so that they are not visible to people walking by
- Properly dispose of old equipment, storage devices, disks, CD, etc.